VIII kadencja

SEJM
RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

- **Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 40)**
- **Komisji do Spraw Energii i Skarbu Państwa (nr 38)**

z dnia 3 listopada 2016 r.

Pełny zapis przebiegu posiedzenia

Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 40)

Komisji do Spraw Energii i Skarbu Państwa (nr 38)

3 listopada 2016 r.

Komisje: Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz do spraw Energii i Skarbu Państwa obradujące pod przewodnictwem posła **Pawła Pudłowskiego (N)**, przewodniczącego Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, rozpatrzyły:

– informację Ministra Energii o bezpieczeństwie sieci komputerowych w obiektach infrastruktury energetycznej.

W posiedzeniu udział wzięli: **Andrzej Piotrowski** podsekretarz stanu w Ministerstwie Energii wraz ze współpracownikiem, **Piotr Januszewicz** zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji, **Wojciech Trusz** naczelnik Wydziału Rynku Cyfrowego i Nowych Technologii Departamentu Gospodarki Elektronicznej Ministerstwa Rozwoju wraz ze współpracownikiem, **Jarosław Kowalik** naczelnik Wydziału Bezpieczeństwa Infrastruktury Teleinformatycznej Departamentu Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji, gen. **Marek Bieńkowski** dyrektor Departamentu Porządku i Bezpieczeństwa Najwyższej Izby Kontroli wraz ze współpracownikiem, **Andrzej Politowski** główny specjalista w Rządowym Centrum Bezpieczeństwa, prof. dr hab. inż. **Marian Noga** prezes Polskiego Towarzystwa Informatycznego, **Michał Lewczuk** wiceprezes ENERGA Informatyka i Technologie Sp. z o.o. wraz ze współpracownikiem, **Tomasz Góreczny** dyrektor Biura Bezpieczeństwa Energa S.A., **Włodzimierz Dobrowolski** przedstawiciel GAZ-SYSTEM S.A., **Leszek Wojdalski** dyrektor Departamentu Strategii IT PGE S.A., **Marek Frąckiewicz** dyrektor ds. Informatyki PKN Orlen S.A., **Eryk Kłossowski** prezes Polskie Sieci Elektroenergetyczne S.A. wraz ze współpracownikami oraz **Piotr Urbańczyk** przedstawiciel Tauron Polska Energia S.A.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Ewa Gast**, **Wiesław Kozioł**, **Iwona Kubaszewska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Paweł Pudłowski (N):

Dzień dobry. Witam panie i panów posłów oraz zaproszonych gości. Bardzo proszę o zajęcie miejsc.

Otwieram posiedzenie Komisji obradujących wspólnie – tj. Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Komisji do spraw Energii i Skarbu Państwa.

Stwierdzam kworum obu Komisji.

Porządek dzisiejszego posiedzenia zawiera rozpatrzenie informacji ministra energii o bezpieczeństwie sieci komputerowych w obiektach infrastruktury energetycznej.

Powyższy porządek członkowie Komisji otrzymali. Czy są uwagi do porządku dziennego? Nie słyszę. Stwierdzam, że Komisje przyjęły porządek dzienny posiedzenia bez zmian.

Przystępujemy do realizacji porządku dziennego. Uprzejmie proszę podsekretarza stanu w Ministerstwie Energii – pana Andrzeja Piotrowskiego o przedstawienie informacji.

Podsekretarz stanu w Ministerstwie Energii Andrzej Piotrowski:

Dzień dobry państwu. Andrzej Piotrowski, podsekretarz stanu w ME.

Proszę państwa, przedmiotem dzisiejszego posiedzenia jest kwestia polityki bezpieczeństwa w obiektach infrastruktury sektora energetycznego. Chcę zwrócić państwa uwagę na to, że jest to sprawa wielowątkowa. Ponieważ rozmawiamy w trybie publicznym, to nie chciałbym, żebyśmy wnikali w niektóre rzeczy, które nie powinny być omawiane w tym trybie. Z jednej strony mamy kwestię mechanizmu bezpieczeństwa i kwestię polityk bezpieczeństwa, które są domeną informacji publicznej. Z drugiej strony mamy sferę realizacji poszczególnych działań.

Na dodatek w sektorze energetycznym występuje pewnego rodzaju zróżnicowanie. Z jednej strony mamy sieci elektroenergetyczne, które we współczesnym świecie są sieciami silnie zautomatyzowanymi. Oznacza to, że mogą być potencjalnie elementem zagrożonym w wyniku działań destrukcyjnych w sferze IT.

Mamy też typowe rozwiązania tzw. *back office*, czyli zaplecza teleinformatycznego, w którym poszczególne koncerny energetyczne realizują takie same zadania jak szereg innych przedsiębiorstw. Mianowicie prowadzą swoją księgowość, rozliczenia z klientami, wspomagają procesy operacyjne i biurowe. To też są systemy, które mogą podlegać zaburzeniom ze strony wrogo nastawionych osób czy chcących poczynić jakieś szkody – mniejsza o motywacje. Tym niemniej klasa skutków zagrożeń dla systemów jest różna, jak również różne są procedury z tym związane.

Proszę państwa, polityka bezpieczeństwa w sektorze energii jest elementem, który kształtujemy w tej chwili dla całego sektora, co nie zmienia faktu, że poszczególne przedsiębiorstwa nie działają pierwszy dzień i mają opracowane swoje własne polityki. Do dzisiejszego dnia, odpukać, nie było jakiś większych problemów. Jednak to nie zmienia faktu, że mamy do czynienia z pewnego rodzaju wyścigiem zbrojeń. To, że coś się nie zdarzyło, nie oznacza, że coś złego nie może się wydarzyć za chwilę.

W związku z tym, obecnie w resorcie rozważamy nie tylko kwestię przeprowadzenia audytu bezpieczeństwa, mającego na celu sprawdzenie skuteczności polityk, które państwo macie opisane w dostarczonym, dość obszernym materiale. Nie chciałbym w tej chwili wnikać w omawianie poszczególnych elementów, ponieważ zajmie nam to prawdopodobnie kilka godzin i niekoniecznie dostarczy dalej idących wniosków.

Natomiast chciałbym zwrócić uwagę, że analiza dotychczasowego podejścia do bezpieczeństwa nie wyczerpuje zagrożeń, które dostrzegamy. Musimy zdawać sobie sprawę z eskalacji i z tego, że mogą być wykorzystane również informacje na poziomie meta, to znaczy, że mogą zostać wykorzystane rzeczy, które do tej pory nie były brane pod uwagę. Nie chcę tutaj uciekać się do przykładów filmów grozy, w których takie scenariusze są przedstawiane bardzo chętnie. Musimy liczyć się z tym, że ktoś – wiedząc o słabych punktach technicznych np. sieci elektroenergetycznej – będzie w stanie wywołać zagrożenie zupełnie w innym miejscu. Na przykład włamie się do systemów klimatyzacyjnych i zwiększy w tym obszarze pobór energii w momencie szczytowego jej zużycia, co spowoduje dalej idące konsekwencje, np. przegrzanie jakiś elementów i ich uszkodzenie.

W związku z tym musimy działać coraz bardziej rozważnie i chronić informacje również nie tylko co do ich treści, ale również co do samego faktu, że przekazywana była informacja z określoną gęstością.

W sprawozdaniu nie zostało to ujęte, ale w tej chwili prowadzimy konsultacje w ramach resortu dotyczące sieci komunikacji kryzysowej. Chcemy faktycznie znaleźć rozwiązanie, które będzie rozwiązaniem wspólnym dla podmiotów elektroenergetycznych, które z jednej strony pozwoli na sprostanie wymogom dyspozycyjności tego typu sieci niezależnie od miejsca, w którym konieczna jest komunikacja. Przypominam, że energetyka ma sporą część swoich zasobów w miejscach, gdzie np. telefonia komórkowa słabo sobie radzi. To nie jest przypadek, że tzw. główne punkty zasilające budowane są na obszarach oddalonych od miast. Nikt nie chciałby żyć w pobliżu pola izolatorów, transformatorów i krzyżowania się linii wysokiego napięcia – widzimy to po reakcjach obywateli na ogłoszenie o przeprowadzeniu linii – a co dopiero na tego typu instalacje.

Tym niemniej w tym miejscu bardzo potrzebne są działania związane z komunikacją, zarówno między ekipami naprawczymi, jak i centralą poszczególnych ośrodków. W tej chwili dysponujemy systemami rozproszonymi, nieujednoliconymi, w związku z tym kosztownymi w eksploatacji. Część z nich jest systemami analogowymi, co sta-

nowi paradoksalnie pewien czynnik bezpieczeństwa. Jednak sposób organizacji sieci jest czasami dziwny. Są to zorganizowane przez nasze podmioty, stowarzyszenia. Musimy to w pewien sposób uporządkować. Tutaj już nie ma nikt wątpliwości, że zostanie to zorganizowane inaczej, w sposób logiczny.

Równocześnie musimy rozstrzygnąć dylemat, czy iść w rozwiązania, które w tym momencie spełniają oczekiwania co do funkcjonalności poszczególnych operatorów, ale wiadomo o nich, że w ciągu najbliższych lat staną się technicznie archaiczne, czy znaleźć na rynku rozwiązanie, które jednakże jeszcze nie spełnia wszystkich wymogów, ponieważ jest we wczesnej fazie rozwoju. Na przykład takie rozwiązanie odwołuje się do tych samych technik komunikacyjnych, co telefonia komórkowa w swoim najnowszym wydaniu LTE.

Tym niemniej tam to jest usługa publiczna, której stawiano trochę inne wymagania. Są przygotowywane nowe wersje standardu. Tylko zaznaczam, że nie ma jeszcze tego standardu, a co dopiero konkretnych urządzeń.

W tym trudnym momencie przełomu technologicznego musimy znaleźć rozwiązanie, żeby można było skorzystać z usług komunikacyjnych już obecnie, a równocześnie nie wydać dużej ilości pieniędzy na rzeczy, które będziemy za chwilę wycofywać. Tutaj mówię głównie o komunikacji głosowej.

Pozostaje jeszcze cała sfera komunikacji związanej z transmisją danych między urządzeniami w ramach sieci, którą obsługują nasi operatorzy, ale również komunikacji z urządzeniami użytkowników energii. To jest kwestia zarówno komunikacji z licznikami energii, jak i kwestia wprowadzania nowych rozwiązań związanych ze sterowaniem popytem. Urządzenie może zostać zdalnie uruchomione zgodnie z zawartym kontraktem w momencie, kiedy występuje obniżony poziom poboru energii w sieci. Czynności, które to urządzenie wykonuje, najlepiej żeby zostały wykonane właśnie w takim momencie. Albo może wystąpić odwrotna sytuacja. W momencie, kiedy dane urządzenie nie musi stale pracować, a występuje zwiększone zapotrzebowanie na energię elektryczną, to niektóre urządzenia zostaną wyłączone.

Przestrzegam, bo niektórzy nazywają to „wirtualną elektrownią". To jest trochę niefortunne sformułowanie, bo prąd nie jest wytwarzany. Energia elektryczna jest oszczędzana, ale ostatecznie efekt jest taki, jakby faktycznie postawiono kolejny blok elektrowni. Stąd wzięła się wspomniana nazwa marketingowa.

Proszę państwa, takie rozwiązania są bardzo ważne, bardzo cenne, ale zarazem wprowadzają nowy obszar potencjalnych niebezpieczeństw. Pracujemy właśnie nad tym, żeby zredukować możliwość ingerencji w te rozwiązania przez osoby niepowołane. Nie do zera, bo to byłoby stwierdzeniem bardzo bałamutnym, że wyeliminowaliśmy wszelkie niebezpieczeństwa. Pragniemy, aby niebezpieczeństwo było na poziomie nadającym się do zaakceptowania przez obywateli.

Jeżeli państwo macie jakieś pytania szczegółowe, w szczególności do przygotowanego dokumentu, to oczywiście jestem gotów na nie państwu odpowiedzieć wspólnie ze współpracownikiem z Departamentu Innowacji i Nowoczesnych Technologii. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję panie ministrze. Domyślam się, że głośność pana wypowiedzi była dostosowana do tajności przedstawionych informacji.

Tak że zachęcam teraz wszystkich państwa do zadawania pytań bądź podzielenia się opinią w tej sprawie. Mówimy o ważnej kwestii dotyczącej krytycznej infrastruktury państwa.

Pamiętamy, że w 2015 r. część sieci energetycznej Ukrainy została zainfekowana. Doszło do skutecznego włamania. Stąd dzisiejsze posiedzenie. Dlatego tym bardziej oczekuję państwa aktywności w tym zagadnieniu, bo jest to ważne dla Polski. Bardzo proszę.

Poseł Wojciech Zubowski (PiS):

Dziękuję panie przewodniczący.

Szanowni państwo, wracając do sprawy, o której mówił pan minister. Podczas chociażby ostatniego posiedzenia Sejmu, niektórzy parlamentarzyści zorientowali się, że nie działał Twitter i kilka innych popularnych aplikacji. Było to związane m.in. z atakiem,

do którego został użyty tzw. Internet rzeczy – czyli inteligentne urządzenia, które w zasadzie wchodzą do naszych domów.

Zdając sobie sprawę z tego, że nie o wszystkim możemy mówić, chciałbym jeszcze spytać, jak wygląda sprawa odnośnie pozyskiwania doświadczenia i wiedzy dotyczącej radzenia sobie z tego typu niebezpieczeństwami od naszych sąsiadów? Czy występuje wymiana informacji z odpowiednimi ministerstwami innych krajów? Czy są wzorce, z których możemy czerpać? Dziękuję. To wszystko.

Przewodniczący poseł Paweł Pudłowski (N):

Dziękuję bardzo. Czy są jakieś dodatkowe pytania bądź komentarze? Nie słyszę. Pozwolę sobie zadać kilka pytań.

W dobrze przygotowanym materiale, który państwo nam przedstawiliście, nie były wyraziste następujące kwestie. Pragnę zapytać, czy każda ze spółek przeszła wewnętrzny audyt bezpieczeństwa oraz jaki był jego rezultat? A jeśli nie wszędzie był przeprowadzony, to czy państwo planujecie takie audyty? Ponadto które z wymienionych spółek posiadają już certyfikat ISO-27001, który jest istotny w kwestiach bezpieczeństwa?

Bardzo proszę.

Dyrektor Departamentu Porządku i Bezpieczeństwa Najwyższej Izby Kontroli gen. Marek Bieńkowski:

Bardzo dziękuję panie przewodniczący. Marek Bieńkowski. Dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli.

Moja obecność na posiedzeniu Komisji obradujących wspólnie nie jest przypadkowa. Chcę państwu zapowiedzieć – również panu ministrowi – że w porozumieniu z panią minister Streżyńską w przyszłym roku planujemy ogólnopolską kontrolę dotyczącą zabezpieczenia naszego państwa przed zagrożeniami antyterrorystycznymi, również jeśli chodzi o systemy teleinformatyczne w infrastrukturze krytycznej.

Chcę pana przewodniczącego i Wysoką Komisję poinformować, że już jesteśmy po kontroli i niezbyt krzepiących wynikach dotyczących zabezpieczenia systemów teleinformatycznych w instytucjach ważnych dla funkcjonowania państwa, m.in. w Ministerstwie Spraw Wewnętrznych i Administracji, w Straży Granicznej, w Narodowym Funduszy Zdrowia, w Ministerstwie Sprawiedliwości – np. systemie elektronicznych ksiąg wieczystych i tym podobnych instytucjach.

W odniesieniu do ostatniego pytania pana przewodniczącego, okazuje się, że ustalenia naszej kontroli świadczą o tym, że wiele instytucji – niemal wszystkie, które skontrolowaliśmy podczas ostatniej kontroli – rzeczywiście legitymują się certyfikatem ISO-2001. Problem polega jednak na tym, że po audycie uzyskania tego certyfikatu następuje dramatyczna pustka w konkretnych działaniach. Oby ustalenia naszej kontroli nie sprawdziły się w zabezpieczeniach systemów teleinformatycznych i infrastruktury krytycznej.

W zasadzie opierają się na jednym, niezbyt krzepiącym twierdzeniu. Otóż brakuje samoświadomości decydentów. Szereg problemów związanych z zabezpieczeniem niezwykle ważnych sieci teleinformatycznych pozostawiony jest informatykom, którzy ze względu na stosunkowo niskie usytuowanie w strukturach organizacji, w których funkcjonują, powoduje, że systemy są niewydolne.

Dlatego też pozwalam sobie zabrać głos, awizując państwu z jednej strony kontrolę, która zapewne zainteresuje państwa Komisje, a z drugiej strony ustalenia, które są za nami i które niestety krzepiące nie są. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Dziękuję bardzo. Panie ministrze, czy można prosić o odpowiedź na pytania?

Podsekretarz stanu w ME Andrzej Piotrowski:

Proszę państwa, więc jeśli chodzi o audyty, to grupa audytów związana z bezpieczeństwem była przeprowadzana zanim jeszcze powstało ME. Jeszcze nie robiliśmy nowej edycji audytów i przeglądów po powstaniu ME. Zamierzamy przystąpić na początku przyszłego roku do – nazwijmy to – generalnego sprawdzenia procedur bezpieczeństwa oraz dostosowania ich do zasad i wymogów norm.

Chcę zwrócić uwagę na jeden bardzo istotny aspekt. Bardzo często normy ISO służą do zasłaniania się przed faktycznie podejmowanymi działaniami. Normy ISO przewidują reguły postępowania, a nie samo postępowanie. W dużej mierze opierają się o to, że poszczególne podmioty muszą same sobie określić, jak u nich wdrożenie danej normy powinno wyglądać. Niestety, wspomniana część rynku cechuje się tym, że akceptuje się sytuację, w której niekoniecznie bada się wdrożenie norm przez podmioty prywatne. Tak naprawdę sprawdza się, czy ktoś stworzył papier, na którym napisał, co będzie robił. W związku z tym w szczególnych przypadkach bezpieczeństwo tak uzyskane może być iluzoryczne.

Zwrócę uwagę na to, że to jest ten sam sposób podejścia, który funkcjonował przy normach jakości. Normy jakości gwarantowały tylko jedno: że przedsiębiorstwo będzie działało w sposób uporczywie powtarzający tę samą procedurę, nawet jeżeli jest ona błędna. To samo może nastąpić w przypadku bezpieczeństwa. W związku z tym tak naprawdę musimy sprawdzić nie tyle, czy wypełniane są normy, ile czy poziom bezpieczeństwa, poziom myślenia o bezpieczeństwie jest właściwy.

W tym miejscu odniosę się do tego, co powiedział pan z NIK. Wydaje się rzeczą bardzo właściwą, żeby specjalista z danej dziedziny zajmował się tym, na czym się zna, w odróżnieniu od prezesa, który często jest ekonomistą, prawnikiem czy osobą o wykształceniu np. elektroenergetycznym, co niekoniecznie jest tożsame ze znajomością systemów. To jest raczej kwestia wytworzenia ścieżki decyzyjnej, gdzie głos specjalisty jest wystarczająco ważny. Czasami traktuje się, że ten specjalista powinien być członkiem zarządu. To nie musi być skuteczne. Zarządy spółek są ciałami kolegialnymi i trudno zakładać, że informatycy będą mieli przewagę głosów. Wtedy tworzylibyśmy spółki informatyczne, a nie spółki sektora energetycznego.

Tak więc podkreślam: tutaj jest ważne, żeby były osoby kompetentne w firmie, i żeby te osoby kompetentne funkcjonowały w otoczeniu, które dostarczy możliwości realizowania zadań przyczynowo-skutkowych. Jeżeli jest zagrożenie, to odpowiada mu procedura, w której to zagrożenie jest eliminowane w sposób skuteczny. Będę wdzięczny, jeżeli NIK będzie podzielał tego typu wizję, a nie instrumentalne podejście, które zakłada, że w zarządzie musi być informatyk. Informatyk może być również po uczelni ekonomicznej i znać się doskonale na regułach definiowania baz danych finansowo-księgowych. Musi to być osoba o właściwym wykształceniu do danego tematu.

Natomiast bardzo cieszę się, że NIK przeprowadził ogólnopolską kontrolę. Sądzę, że jest to ważne. Zazwyczaj takie kontrole pozwalają dostrzec rzeczy, których ludzie pracujący ze spółkami na bieżąco, funkcjonujące w tym otoczeniu, nie dostrzegają, bo są one tak oczywiste, że trudno je dostrzec.

Proszę państwa, jeszcze na koniec kwestia wymiany informacji pomiędzy państwami. Otóż z jednej strony w sektorze informatycznym czy telekomunikacyjnym istnieje, może nie do końca sformalizowany, ale dość sprawnie funkcjonujący mechanizm, w którym dostawcy poszczególnych rozwiązań komunikują się między sobą. Utrzymują m.in. w sieci rozległe firewalle czy zabezpieczenia. Są organizacje o statusie organizacji społecznych, które monitorują pojawiające się niebezpieczeństwa. Stąd mamy informacje o tym, że następowały w poszczególnych sieciach włamania czy incydenty, chociaż zazwyczaj opinii publicznej nie są przekazywane zbędne szczegóły, żeby nikogo nie inspirować.

Natomiast oczywiście nie można wykluczyć, że w gronie osób zainteresowanych pokazaniem swoich umiejętności znajdują się osoby, które w ciągu dnia pracują w firmach. Trzeba pamiętać, że jednym z największych zagrożeń dla bezpieczeństwa systemów cybernetycznych jest człowiek, który pracuje w danej firmie. Jest to osoba, która podatna jest na różne motywacje, czasem finansowe, czasem polityczne. Tak że musimy tworzyć system, w którym współpracują zarówno informatycy, osoby od telekomunikacji, służby bezpieczeństwa, jak i podmioty z zewnątrz, takie jak NIK, które co jakiś czas przyjrzą się krytycznym okiem i wskażą, które rzeczy są poukładane w nieprawidłowy sposób, a więc mogą prowadzić do zagrożeń czy niebezpieczeństw. Nawet, jeżeli ich opinia w danym momencie nie będzie trafna, to wywoła co najmniej dyskusję i przemyślenia, czy to faktycznie jest trafne, czy być może trochę na wyrost.

Jeśli chodzi natomiast o zagrożenia w sieci ukraińskiej, to one miały trochę inną naturę. Polegały na wyłączeniu pewnych bloków energetycznych w sieci sterowanej w systemach analogowych. Tak jak wiemy w tej chwili, że był to jeden z problemów, który został odziedziczony historycznie po układzie politycznym. Znacznie lepszą dokumentacją o sieciach energetycznych Ukrainy dysponują Rosjanie niż Ukraińcy. W związku z tym procedury bezpieczeństwa i ewentualne procedury naprawcze czasem rodzą trudności, których nasi sąsiedzi nie przewidywali. Na szczęście u nas od dłuższego czasu jest ciągłość. Stąd liczymy, że tego typu problemy u nas nie wystąpią, chociaż licho nie śpi.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję panie ministrze.

Mam pytanie, czy na sali są przedstawiciele firm? Zostali oni zaproszeni na dzisiejsze posiedzenie – m.in. z PSE, GAZ-SYSTEM, Energa, Orlenu. Czy są państwo obecni? Jesteście, więc bardzo się cieszę.

Czy moglibyście ustosunkować się do wypowiedzi pana dyrektora NIK o zaniku alertu po sprawdzeniu, po audycie, po certyfikacie, czy rzeczywiście obserwujecie coś takiego, że w momencie, kiedy trwa sprawdzenie, to wszystkie ręce na pokład, a potem sprawy się nie odbywają w taki sposób, w jaki powinny?

Prezes Polskie Sieci Elektroenergetyczne S.A. Eryk Kłossowski:

W imieniu Polskich Sieci Elektroenergetycznych, Eryk Kłossowski, prezes zarządu.

Jeżeli chodzi o nasze podejście do bezpieczeństwa, to ono jest oparte o zasady ciągłego doskonalenia. A zatem uzyskanie audytu ISO-27001 w żaden sposób nie uprawnia nas do twierdzenia, że jest już bezpiecznie i możemy spocząć na laurach.

Cały czas prowadzimy kolejne audyty. Cały czas korzystamy z wiedzy organizacji branżowych, np. ENCO, grupującej wszystkich operatorów systemów przesyłowych w Europie, a także współpracujemy z nimi w celu wykrywania kolejnych luk, kolejnych podatności oraz kolejnych dróg cyberataków, przy pomocy których można destabilizować pracę całej infrastruktury elektroenergetycznej.

Tak że w tej kwestii uzyskanie certyfikatu w żadnym wypadku nas nie usypia.

Przewodniczący poseł Paweł Pudłowski (N):

Wszyscy z państwa macie podobne odczucia, tak? Bardzo cieszę się z sygnalizowanej kontroli NIK. Chce pan odnieść się do tego? Bardzo proszę panie dyrektorze.

Dyrektor departamentu NIK gen. Marek Bieńkowski:

Nie chcę państwu zabierać czasu. Cieszę się, że jesteśmy zgodni. Mówię, że przychodzimy do państwa, żeby państwu pomóc, a państwo mówicie, że nie możecie się na nas doczekać. Tak więc w tej kwestii panuje pełna zgoda.

Proszę państwa, natomiast źle zostałem zrozumiany przez pana ministra i dlatego chciałem krótko to sprostować. W ustaleniach kontroli, która już jest za nami – mam nadzieję, że tych ustaleń nie potwierdzimy w przyszłej kontroli. Rzecz polega na tym, że absolutnie nie jest naszą tezą, żeby informatyk wchodził do zarządu czy współdecydował w firmie. To już jest kwestia wewnętrzna podmiotu.

Natomiast stwierdziliśmy następujące przypadki, chcę być w tym zakresie bardzo precyzyjny. Otóż praktycznie, jeszcze raz powtórzę, wszystkie instytucje publiczne, w których byliśmy, przed naszym przyjściem z kontrolą, przeprowadziły audyty i pozyskały certyfikat ISO.

Zgoda panie ministrze, certyfikat to nic innego jak procedury, które dopiero trzeba wprowadzić. Słaby punkt polega na tym, że brak samoświadomości decydentów w instytucjach publicznych powodował, że z pozycji specjalisty taki informatyk, który miał status eksperta z zakresu informatyki, miałby wydawać dyspozycje naczelnikom, dyrektorom bądź członkom zarządu. To jest absurdalne. Oczywiście nie miał siły sprawczej. W związku z tym nie twierdzę, że taki ekspert lub informatyk powinien zasiadać we władzach spółki lub innego podmiotu.

Nasz wniosek jest oczywisty, że wprowadzanie procedur, analiza i korekta działań musi być przedmiotem troski całej organizacji, w tym również tych, którzy kierują firmą. Taki był nasz wniosek. Ale absolutnie nie ingerujemy i nie postulujemy, żeby ktokol-

wiek z tego powodu, że jest ekspertem, wchodził do władz spółki. Na tej samej zasadzie moglibyśmy mówić o ochronie informacji niejawnej i szeregu innych dziedzin. Rzecz nie w tym, żeby mnożyć byty w zarządach spółek. To jest niezbyt pocieszające ustalenie, ale jeszcze raz je powtórzę. Trzeba zacząć od samoświadomości tych, którzy decydują o sposobie funkcjonowania organizacji.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję za to dodatkowe wyjaśnienie.

Mam pytanie do spółek. W jaki sposób państwo podchodzicie do wspomnianego słabego elementu infrastruktury, jakim jest człowiek, czyli *interface* białkowego? Co państwo robicie, żeby mieć pewność, że jesteście „szczelni"?

Jak nikt z państwa nie chce zabrać głosu, to będę wywoływał po kolei. Tak że lepiej się zgłosić, jeżeli ktoś czuje się wystarczająco pewnie.

Chodzi mi o szkolenia. Jak często są one przeprowadzane? Czy są kończone egzaminem? Czy prowadzicie państwo testowe sprawdzanie systemu? O te rzeczy pytam.

Dyrektor Departamentu Teleinformatyki Polskich Sieci Elektroenergetycznych Grzegorz Bojar:

Dzień dobry. Grzegorz Bojar. Polskie Sieci Elektroenergetyczne. Jestem dyrektorem Departamentu Teleinformatyki, czyli właśnie tym człowiekiem, który rzekomo ma za mało do powiedzenia w firmie.

Rzeczywiście element ludzki jest jednym z trudniejszych. Większość życia przepracowałem w korporacjach prywatnych, zwłaszcza zagranicznych. W spółkach państwowych element ludzki jest jeszcze bardziej trudny, gdyż są zmniejszone możliwości zarządzania nim.

Natomiast muszę powiedzieć, że na to, co zostało powiedziane o kontrolach przeprowadzonych w różnych podmiotach Skarbu Państwa, warto stwierdzić, że – z mojego doświadczenia i wiedzy – spośród reguł o niskim poziomie świadomości bezpieczeństwa wyłamują się spółki elektroenergetyczne. Po prostu w tych spółkach ludzie mają bardzo wysoki poziom świadomości potrzeby bezpieczeństwa teleinformatycznego i cyberbezpieczeństwa. To wynika z różnych rzeczy. Rzeczywiście w większości spółek elektroenergetycznych, w których ostatnio poznałem ludzi, są zatrudnieni wysokiej klasy fachowcy. Tyle chciałem przekazać.

Przewodniczący poseł Paweł Pudłowski (N):

Dziękuję bardzo. Z pytaniem zgłasza się pan przewodniczący. Bardzo proszę.

Poseł Krzysztof Sitarski (Kukiz15):

Dziękuję panie przewodniczący.

Mam pytanie do pana ministra. Czy w ministerstwie jest komórka koordynująca informacje o ewentualnych zagrożeniach teleinformatycznych względem sprzedawców z obowiązanych sieci przesyłowych? Czy po prostu istnieje taka komórka? To jest jedno pytanie.

Drugie, czy były odnotowane próby zdestabilizowania sieci teleinformatycznej? Być może takie próby były, a taka informacja nie doszła. Czy były zapytania względem przedsiębiorców, zwłaszcza dotyczące czynnika ludzkiego, o którym tutaj wcześniej była mowa? Czy taka próba była w jakikolwiek sposób podjęta? Czy komórka monitorująca to stwierdziła? Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Dziękuję. Czy są jakieś dodatkowe pytania? Jeśli nie, to zamykamy listę pytań i na tym zakończymy. Bardzo proszę o odpowiedź.

Podsekretarz stanu w ME Andrzej Piotrowski:

Panie przewodniczący, centra zarządzania kryzysowego są zlokalizowane tam, gdzie najlepiej spełniają swoją rolę, czyli u poszczególnych operatorów, czy to sieci przesyłowej, czy to sieci dystrybucyjnej. Oczywiście skala i kompetencje centrum zależą od skali działalności operatora. Są bardzo mali operatorzy, u których tego typu usługi są szczątkowe, ale i potencjalne zagrożenia są niewielkie.

Natomiast jeżeli chodzi o samo ministerstwo, to zaznaczam, że jest to młode ciało, które zajmuje się energetyką od niedawna. Do tej pory nie tworzyliśmy wyspecjalizowanej komórki z tego względu, że dopiero zaczynamy się zajmować kwestiami inteligentnej sieci energetycznej, wprowadzając nowe regulacje.

Tym działaniom towarzyszyło pozyskiwanie personelu dla ministerstwa. To jest bardzo trudne, bo ministerstwo zostało utworzone na bardzo skromnych zasobach, wydzielonych z Ministerstwa Gospodarki, gdzie też nie było tego typu osób. W związku z tym każdy kolejny etap jest problemem. Akurat specjaliści z obszaru *cybersecurity*, nie wiem czemu, ale niekoniecznie chcą pracować za pieniądze, które jest w stanie im zaoferować ministerstwo. Wychodzimy z założenia, że koordynacja tak, natomiast bezpieczeństwo musimy lokować tam, gdzie są podmioty, które mogą dostosować płace do natury komplikacji występujących zagadnień.

Oczywiście każda sieć teleinformatyczna jest przedmiotem – może ustawicznych to przesada, ale powtarzających się ataków. Szczególnie ta, do której jest dostęp z zewnątrz, a do części rozwiązań funkcjonujących w sektorze energetycznym właśnie jest zagwarantowany dostęp z zewnątrz. Jest to pewnego rodzaju wyścig zbrojeń. O szczegółach tego dotyczących można w zasadzie poczytać w jakiś biuletynach organizacji zajmujących się wymianą informacji o bezpieczeństwie sieciowym. System elektroenergetyczny nie jest systemem narażonym bardziej – na szczęście jak tej pory – niż np. sieci banków czy innych podmiotów, gdzie występują ciekawe obiekty do zdestabilizowania albo uzyskania korzyści materialnych.

W związku z tym, jako ministerstwo, nie staramy się ani w szczególny sposób zbierać informacji do momentu, dopóki nie mamy powodów osądzać, że występuje jakaś eskalacja. Tak jak w pozostałych sektorach odbywają się ataki, głównie polegające na wszystkim znanym zmasowanym adresowaniu określonych serwerów po to, żeby wykluczyć do nich dostęp. Na szczęście na tego typu problemy, które parę lat temu wydawały się być trudne do rozwiązania, producenci routerów znaleźli sposoby i sektor sobie z tym radzi.

Natomiast faktycznie spora część sieci sektora jest wydzielona, ma jedynie pojedyncze punkty styku z siecią i właśnie te punkty są pilnie strzeżone.

Tak że nie wiem, na ile odpowiedziałem na pana pytania.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo uprzejmie dziękuję za odpowiedź oraz za państwa obecność.

Zamykam dyskusję.

Stwierdzam, że porządek dzienny posiedzenia został wyczerpany.

Zamykam posiedzenie Komisji.

Protokół posiedzenia z załączonym zapisem jego przebiegu będzie do wglądu w sekretariatach obu Komisji, w kancelarii Sejmu. Miłego wieczoru.